United Nations A/C.2/57/L.10

General Assembly

Distr.: Limited
18 October 2002

Original: English

Fifty-seventh session
Second Committee
Agenda item 84 (c)
Macroeconomic policy questions: science and technology for development

Japan and United States of America: draft resolution

Creation of a global culture of cybersecurity

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the digital economy,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Further aware that technology alone cannot ensure cybersecurity and that a priority must be given to cybersecurity planning and management throughout society,

Recognizing that, appropriate to their roles, Governments, businesses, other organizations and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures, and must assume responsibility and take steps to enhance the security of those information technologies,

Noting that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all computer users,

Noting the work of international and regional organizations on enhancing cybersecurity and the security of information technologies, including the Statement on the Security of Information and Communications Infrastructures, adopted at the Fifth Asia-Pacific Economic Cooperation Ministerial Meeting on Telecommunications and

02-64804 (E) 181002

Information Industry, which was held in Shanghai, China, on 29 and 30 May 2002, the Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, adopted by the Council of the Organization for Economic Cooperation and Development on 25 July 2002, and the document entitled "Network and information security: proposal for a European policy approach", issued by the Commission of the European Communities on 6 June 2001 and transmitted to the European Council, the European Parliament, the European Economic and Social Committee, and the Committee of the Regions,

1. *Adopts* the principles annexed to the present resolution with a view to creating a global culture of cybersecurity;

2. *Invites* Member States to take into account these principles in their efforts to develop, throughout their societies, a culture of cybersecurity in the application and use of information technologies;

3. *Requests* Member States to take these principles and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva in December 2003.

Annex

Principles for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ("participants") must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary principles:

(a) *Awareness*. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(b) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(c) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information sharing and cooperation;

(d) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(e) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(f) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to

encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(g) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(h) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(i) *Reassessment*. Participants should review and reassess the security of information systems and networks, and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.